

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

HONG-SAM KIM, *et al.*

Serial No.: *To be assigned*

Examiner: *To be assigned*

Filed: 8 February 2001

Art Unit: *To be assigned*

For: *METHOD FOR AUTOMATICALLY VERIFYING SECURITY CODE OF
COMPUTER SYSTEM OPERATED BY REMOTE CONTROLLER*

CLAIM OF PRIORITY UNDER 35 U.S.C. §119

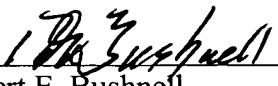
The Assistant Commissioner
for Patents
Washington, DC 20231

Sir:

The benefit of the filing date of the following prior foreign applications, Korean Priority No. 2000-10443 (filed in Korea on 2 March 2000), and filed in the U.S. Patent and Trademark Office on 8 February 2001 is hereby requested and the right of priority provided in 35 U.S.C. §119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application.

Respectfully submitted,


Robert E. Bushnell
Reg. No.: 27,774
Attorney for the Applicant

1522 "K" Street, N.W., Suite 300
Washington, D.C. 20005-1202
202 408-9040

Folio: P56295
Date: 02/08/2001
I.D.: REB/mnf

#4
J1033 U.S. PTO
09/776730
02/08/01

Best Available Copy

J1033 U.S. PTO

09/778730



대한민국 특허청

KOREAN INDUSTRIAL
PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

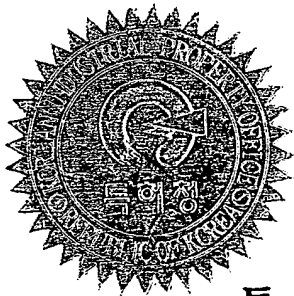
This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Industrial
Property Office.

출원번호 : 특허출원 2000년 제 10443 호
Application Number

출원년월일 : 2000년 03월 02일
Date of Application

CERTIFIED COPY OF
PRIORITY DOCUMENT

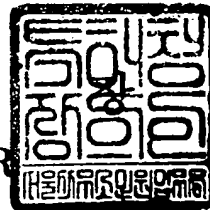
출원인 : 삼성전자 주식회사
Applicant(s)



2000 년 05 월 19 일

특 허 청

COMMISSIONER



【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0008
【제출일자】	2000.03.02
【발명의 명칭】	리모트 컨트롤러로 구동되는 컴퓨터 시스템의 자동 암호 확인 방법
【발명의 영문명칭】	AN AUTOMATIC SECURITY CODE VERIFYING METHOD OF A COMPUTER SYSTEM OPERATED BY A REMOTE CONTROLLER
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	임창현
【대리인코드】	9-1998-000386-5
【포괄위임등록번호】	1999-007368-2
【대리인】	
【성명】	권혁수
【대리인코드】	9-1999-000370-4
【포괄위임등록번호】	1999-056971-6
【발명자】	
【성명의 국문표기】	김홍삼
【성명의 영문표기】	KIM,HONG SAM
【주민등록번호】	640613-1624721
【우편번호】	449-840
【주소】	경기도 용인시 수지읍 상현리 1번지 동보2차아파트 101동 1302호
【국적】	KR
【발명자】	
【성명의 국문표기】	이병재
【성명의 영문표기】	LEE,BYUNG JAE
【주민등록번호】	641119-1520311
【우편번호】	442-470

【주소】 경기도 수원시 팔달구 영통동 황골마을 쌍용APT 247동
1603호

【국적】 KR

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대
리인 임창
현 (인) 대리인
권혁수 (인)

【수수료】

【기본출원료】	20 면	29,000 원
【가산출원료】	7 면	7,000 원
【우선권주장료】	0 건	0 원
【심사청구료】	0 항	0 원
【합계】		36,000 원

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】**【요약】**

여기에 개시된 컴퓨터 시스템은, 이를 원격으로 조정하기 위한 원격제어신호를 발생하는 리모트 컨트롤러 및 상기 리모트 컨트롤러로부터 발생하는 원격제어신호를 받아들이는 원격제어신호 수신부, 그리고 리모트 컨트롤러에 의한 다양한 원격제어동작을 실행하는 셀 프로그램을 포함한다. 상기 셀 프로그램은, 컴퓨터 시스템이 리모트 컨트롤러에 의해서 대기상태에서 정규상태로 복귀할 때 암호확인 작업이 수행되면 리모트 컨트롤러로부터 전송되는 암호를 자동으로 입력해 주는 역할을 수행한다. 따라서, 대기상태에서 정규상태로 복귀할 때 사용자가 키보드와 같은 입력장치를 통해서 입력해야했던 암호 입력 작업을 자동으로 수행함으로써 사용자의 편리를 도모할 수 있다.

【대표도】

도 7

【명세서】

【발명의 명칭】

리모트 컨트롤러로 구동되는 컴퓨터 시스템의 자동 암호 확인 방법{AN AUTOMATIC SECURITY CODE VERIFYING METHOD OF A COMPUTER SYSTEM OPERATED BY A REMOTE CONTROLLER}

【도면의 간단한 설명】

도 1은 본 발명의 제1 실시예에 따른 리모트 컨트롤러를 구비한 컴퓨터 시스템의 외관을 보여주는 사시도;

도 2는 도 1에 도시된 리모트 컨트롤러 및 원격제어신호 수신부를 포함하는 컴퓨터 시스템의 구성을 개략적으로 보여주는 블록도;

도 3은 도 2에 도시된 리모트 컨트롤러의 구성을 간략히 보여주는 도면;

도 4는 도 2에 도시된 원격제어신호 수신부의 구성을 간략히 보여주는 도면;

도 5는 도 2에 도시된 컴퓨터 시스템의 구성을 계층적으로 보여주는 도면;

도 6은 전원관리 기능이 있는 컴퓨터 시스템의 전원 상태의 천이를 보여주는 상태도; 그리고

도 7은 본 발명의 제1 실시예에 따른 컴퓨터 시스템이 대기상태에서 정규상태로 복귀될 때 수행되는 암호확인 동작 수순을 보여주는 흐름도;

도 8은 본 발명의 제2 실시예에 따른 멀티유저 컴퓨터 시스템의 개략적인 구성을 보여주는 블록도;

도 9는 도 8의 멀티유저 컴퓨터 시스템의 하드디스크의 메모리 영역을 보여주는 도면; 그리고

도 10은 도 8의 멀티유저 컴퓨터 시스템의 암호확인 동작 수순을 보여주는 흐름도이다.

도면의 주요 부분에 대한 부호의 설명

CONTROLLER 200 : 컴퓨터 시스템 210 : 전원 스위치
250 : PCI-to-ISA 브릿지 251 : 시스템 전원관리부
252 : GPIO 260 : BIOS
280 : 전원 공급장치 293 : 셀 프로그램
300 : 리모트 컨트롤러 400 : 원격제어신호 수신부

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<17> 본 발명은 컴퓨터 시스템에 관한 것으로, 좀 더 구체적으로는 리모트 컨트롤러로 구동되는 컴퓨터 시스템의 자동 암호 확인 방법에 관한 것이다.

<18> 리모트 컨트롤러(remote controller)는 TV, 오디오 플레이어 시스템, 비디오 플레이어 시스템과 같은 많은 전기 제품들의 동작을 제어하기 위해 광범위하게 사용되어 오고 있다. 그리고, 근래 들어서는 보다 편리한 사용자 인터페이스를 위해 컴퓨터 시스템의 동작을 원격으로 제어하기 위해 리모트 컨트롤러가 사용되고 있다.

<19> 최근의 컴퓨터 시스템은, 시스템이 유힬상태(idle state)일 때 특정 구성요

소로의 주 전원을 선택적으로 스위치 오프 하는 에너지 절약 특성을 가진다. 종래의 전원관리회로(power management circuit)는 활동의 표지(sign of activity)로서 키보드(keyboard), 마우스(mouse) 또는 다른 시스템 구성요소들을 모니터링 한다. 그리고 만약 미리 정해진 시간 동안 어떤 활동도 발견되지 않으면 주 공급 전원(main supply power)을 턴 오프 함으로써 상기 시스템을 대기(standby) 모드로 들게 한다. 대기(standby) 모드에서는 저-전류의 대기 전원(standby power)이 공급 전원으로서 대기전원 로직 회로(standby power logic circuit)로 제공된다. 대기전원 로직 회로는 웨이크-업(wake-up) 활동에 응답해서 시스템이 대기 모드(standby mode)에서 빠져 나오게 하는 기능을 수행한다. 전술한 바와 같은 컴퓨터 시스템의 전원관리에 관련된 스펙(specification)은 1996년 12월 22일 발표된 Intel, Microsoft 및 Toshiba에 의한 'Advanced Configuration and Power Interface(ACPI) Specification'에 개시되어 있다.

<20> 일반적으로, 사용자들은 절전이나 보안상의 이유로 컴퓨터 시스템에 암호를 설정해 두고 있다. 예를 들면, 화면보호 상태나 절전 모드에서 사용환경으로 복귀할 때 암호를 확인하는 기능이 그것이다. 컴퓨터 시스템이 슬립(sleep) 상태와 같은 대기상태에서 웨이크(wake) 상태로 전환될 때 암호를 설정해 두지 않으면, 보안이 필요한 장소에서 사용하는 데에는 문제가 발생한다. 이러한 보안상의 문제를 해결하기 위해서 Microsoft사의 Windows 95, 98과 같은 OS 프로그램(Operating System Program)들은, 컴퓨터가 대기상태에서 빠져 나올 때 암호를 확인하는 기능을 제공한다.

<21> 그러나, 컴퓨터 시스템이 대기상태에서 웨이크업(wake-up) 될 때, 상기와 같은 암호 확인 기능이 수행되면 사용자는 직접 키보드를 통해서 암호를 입력해주어야만 한다. 이와 같은 경우, 사용자의 편리한 인터페이스를 위해 리모트 컨트롤러가 제공된다 하더

그러도, 특별한 회로적/소프트웨어적 장치/방법이 제공되지 않는 한 사용자가 직접 키보드를 조작해야만 하는 불편이 따른다. 즉, 보다 편리하게 컴퓨터 시스템을 제어하고자 하는 리모트 컨트롤러의 잇점이 사라지게 되는 것이다. 이 경우, 컴퓨터 시스템에 대한 리모트 컨트롤러로부터의 완전한 원격 조정은 불가능하다 할 수 있다.

<22> 따라서, 암호확인 기능을 가지는 컴퓨터 시스템을 리모트 컨트롤러를 통해 제어하는 경우, 보다 편리하게 암호를 확인할 수 있는 방법이 요구된다.

【발명이 이루고자 하는 기술적 과제】

<23> 본 발명의 목적은 상술한 제반 문제점을 해결하기 위해 제안된 것으로, 리모트 컨트롤러에 의해 동작이 제어되는 컴퓨터 시스템의 보다 편리한 암호확인 방법을 제공하는 데 있다.

【발명의 구성 및 작용】

<24> 상술한 바와 같은 본 발명의 목적을 달성하기 위한 본 발명의 특징에 의하면, 리모트 컨트롤러에 의해 동작이 제어되는 컴퓨터 시스템에 설정된 암호의 확인 방법은, 상기 설정된 암호를 확인하는 기능을 시작하기 위한 암호확인 개시 데이터가 발생하는 단계와, 암호확인 수단으로 암호를 입력하는 단계와, 상기 설정된 암호와 상기 입력된 암호가 일치하는지 여부를 판별하는 단계, 그리고 상기 두 암호가 일치하면 상기 컴퓨터 시스템의 동작 상태를 정규 상태로 전환하는 단계를 포함한다. 상기 입력되는 암호는, 상기 암호확인 개시 데이터가 상기 리모트 컨트롤러에 의해서 발생된 경우, 셀 프로그램에 의해서 상기 암호확인 수단으로 자동으로 입력한다.

<25> (실시예)

<26> 이하, 본 발명의 제1 실시예를 첨부된 도면 제1 내지 제7도를 참조하여 상세히 설명한다.

<27> 본 발명의 신규한 컴퓨터 시스템은, 컴퓨터 시스템을 원격으로 조정하기 위한 원격 제어신호를 발생하는 리모트 컨트롤러 및 상기 리모트 컨트롤러로부터 발생하는 원격 제어신호를 받아들이는 원격제어신호 수신부, 그리고 리모트 컨트롤러에 의한 다양한 원격 제어동작을 실행하는 셸 프로그램을 포함한다. 상기 셸 프로그램은, 컴퓨터 시스템이 리모트 컨트롤러에 의해 대기상태에서 정규상태로 복귀할 때 암호확인 작업이 수행되면 리모트 컨트롤러로부터 전송되는 암호를 자동으로 입력해 주는 역할을 수행한다. 따라서, 사용자가 키보드와 같은 입력장치를 통해서 입력해야했던 암호입력 작업을 자동으로 수행함으로써 사용자의 편의를 도모할 수 있다.

<28> (실시예 1)

<29> 도 1은 본 발명에 의한 리모트 컨트롤러를 구비한 컴퓨터 시스템의 외관을 보여주는 사시도이고, 도 2는 도 1에 도시된 리모트 컨트롤러(300) 및 원격제어신호 수신부를 포함하는 컴퓨터 시스템(200)의 구성을 간략히 보여주는 블록도이다.

<30> 도면을 참조하면, 컴퓨터 시스템(200)은 컴퓨터의 전원 스위치(210)에 의해 구동될 수 있고, 리모트 컨트롤러(300)에 의해서 원격으로 구동될 수 있다. 즉, 상기 리모트 컨트롤러(300)로부터 발생하는 원격제어신호는 컴퓨터 시스템(200) 내에 장착된 원격제어신호 수신부(400)로 전송되어 컴퓨터 시스템(200)의 동작을 제어한다. 상기 원격제어신호 수신부(400)는 컴퓨터 시스템(200)의 PCI-to-ISA 브릿지(250) 내에 장착된 GPIO(General Purpose IO ; 252) 및 셸 프로그램(Shell Program; 293)과 연결된다. 상기 GPIO(252)는, 셸 프로그램(293)으로부터 전송되는 컴퓨터 시스템(200)의 상태 정보를

원격제어신호 수신부(400)로 전달하는 역할을 수행한다. 컴퓨터 시스템(200)의 상태 정보를 받아들이는 원격제어신호 수신부(400)는 전원공급장치(280) 및 전원 스위치(210)에 연결된 시스템 전원관리부(251)를 통해서 전원 관련 원격제어를 수행한다.

<31> 특히, 본 발명에 의한 리모트 컨트롤러(300) 및 이와 쌍을 이루는 원격제어신호 수신부(400)는 정당한 사용자 확인을 위해 서로 동일한 암호를 가진다. 상기 리모트 컨트롤러(300)로부터 발생하는 원격제어 신호에 암호가 같이 전송되며, 이 암호가 일치할 때에만 상기와 같은 리모트 컨트롤러(300)를 이용한 컴퓨터 시스템(200)의 원격 제어가 가능하다.

<32> 도 3은 도 2에 도시된 리모트 컨트롤러(300)의 구성을 간략히 보여주는 도면이다. 도 3을 참조하면, 리모트 컨트롤러(300)는 암호를 저장하기 위한 EEPROM(320), 컴퓨터 원격제어 명령을 발생하기 위한 마이크로컨트롤러(310), 상기 원격제어 명령을 상기 원격제어신호 수신부(400)로 전송하기 위한 원격제어신호 전송회로(330), 그리고 상기 리모트 컨트롤러(300)의 동작 전원을 공급하기 위한 배터리(340)를 포함한다. 마이크로컨트롤러(310)는, 상기 EEPROM(320) 및 원격제어신호 전송회로(330) 사이에 연결되어 원격제어 명령을 발생하고 이를 전송회로(330)를 통해서 전송하는 일련의 동작을 제어하는 기능을 수행한다.

<33> 도 4는 도 2에 도시된 원격제어신호 수신부(400)의 구성을 간략히 보여주는 도면이다. 도 4를 참조하면, 원격제어신호 수신부(400)는 암호를 저장하기 위한 EEPROM(420), 상기 리모트 컨트롤러(300)로부터의 원격제어 명령을 받아들이기 위한 원격제어신호 수신회로(430) 및 상기 EEPROM(420) 및 원격제어신호 수신회로(430) 사이에 연결된 마이크로컨트롤러(410)를 포함한다. 이 마이크로컨트롤러(410)는 원격제어 명령을 받아들이고,

원격제어 명령에 포함된 상기 리모트 컨트롤러(300)의 암호와 상기 EEPROM(420)에 저장된 암호가 일치하는지 여부를 판별하고, 만약 두 암호가 일치하면 상기 원격제어 명령을 수행하도록 제어한다.

<34> 도 5는 도 2에 도시된 컴퓨터 시스템(200)의 구성을 계층적으로 보여주는 도면이다. 도 5를 참조하면, 컴퓨터 시스템(200)은 하드웨어 층(hardware layer ; 500), BIOS 층(BIOS layer ; 510), 운영시스템 층(operating system layer ; 520) 및 어플리케이션 층(application layer ; 530)으로 이루어진 계층적 구조(hierarchical structure)를 가진다.

<35> 상기 하드웨어 층(500)에는 PCI-to-ISA 브릿지(250), 슈퍼 I/O(265) 및 원격제어 신호 수신부(400)가 포함된다. PCI-to-ISA 브릿지(250)는 크게 시스템 전원관리부(251)와 GPIO(252)로 구성되며, 시스템 전원관리부(251)에는 전원공급장치(280) 및 전원 스위치(210)가 공통으로 연결된다.

<36> 상기 BIOS 층(510)에는 BIOS(basic input output system ; 260)가 포함되고, 운영시스템 층(520)에는 Microsoft사의 Windows 95 또는 98과 같은 OS 프로그램(295)과 가상 키보드 드라이버인 VxD(290)가 포함된다. 그리고, 어플리케이션 층(530)에는 상기 VxD(290)와, 프로그램을 자동으로 실행시키는 기능을 수행하는 Launcher(292)로 구성된 셸 프로그램(Shell Program)이 포함되며, 셸 프로그램(293)이 수행하는 기능은 BIOS(260)의 특정 영역에 미리 저장된다.

<37> 그리고, 절전이나 보안상의 이유로 컴퓨터 시스템에 암호를 설정해두고 컴퓨터가 대기상태에서 정규상태로 빠져 나올 때 암호를 확인하는 기능이 제공되는 경우, 상기 셸 프로그램(293)은 리모트 컨트롤러(300)로부터 전송되는 암호를 OS 프로그램(295)으로 직

접 전달한다. 그 결과, 사용자가 키보드로 암호를 입력하지 않아도 암호가 자동으로 입력되어 암호확인 작업이 자동으로 수행된다.

<38> 도 6은 전원관리 기능을 가지는 컴퓨터 시스템의 전원 상태의 천이를 보여주는 상태도이다. 도 6을 참조하면, 컴퓨터 시스템(200)이 가지는 전원 상태는 크게 정규상태(normal state), 대기상태(standby state), 그리고 오프상태(off state)로 구분된다.

<39> 예를 들어, 상기 컴퓨터 시스템(200)이 오프상태(off state)일 때, 상기 리모트 컨트롤러(300)로부터 전송되는 원격제어신호 또는 컴퓨터 시스템(200) 본체에 장착된 전원 스위치(210)에 의해 전원이 인가되면, 상기 컴퓨터 시스템(200)은 부팅이 이루어지고 정규상태가 된다. 반대로, 리모트 컨트롤러(300)로부터 전송되는 원격제어신호 또는 컴퓨터 시스템(200) 본체에 장착된 전원 스위치(210)에 의해 전원이 차단되면, 상기 컴퓨터 시스템의 전원 상태는 정규상태에서 오프상태로 전환된다.

<40> 그리고, 상기 컴퓨터 시스템(200)이 정규상태(normal state)일 때, 만약 리모트 컨트롤러(300)로부터 원격제어신호가 원격제어신호 수신부(400)로 전달되면 상기 컴퓨터 시스템(200)의 전원 상태는 대기상태(standby state)가 된다. 또는, 소정의 시간 동안 키보드(100)와 같은 데이터 입력 장치로부터 데이터의 입력이 이루어지지 않으면, 전원 관리 기능에 의해서 컴퓨터의 전원 상태가 정규상태에서 대기상태로 전환된다. 반대로, 상기 컴퓨터 시스템(200)이 대기상태일 때, 키보드(100), 마우스(110) 또는 리모트 컨트롤러(300) 중 어느 하나의 데이터 입력 장치로부터 데이터가 입력되면, 컴퓨터의 전원 상태는 대기상태에서 정규상태로 전환된다.

<41> 특히, 앞에서 설명한 바와 같이, 절전이나 보안상의 이유로 컴퓨터 시스템에 암호를 설정해두고 컴퓨터가 대기상태에서 정규상태로 빠져나올 때 암호를 확인하는 기능이

제공되는 경우, 컴퓨터 전원상태의 전환은 다음과 같다. 데이터 입력 장치들 중 만약

리모트 컨트롤러(300)의 입력에 의해 정규상태로의 전환이 이루어지는 경우, 상기 셸 프로그램(293)은 리모트 컨트롤러(300)로부터 전송되는 암호를 암호확인 기능을 수행하는 OS 프로그램(295)으로 직접 전달한다. 그 결과, 상기 OS 프로그램(295)은 이 암호를 바탕으로 암호확인 작업을 수행한 후, 컴퓨터의 전원 상태를 정규상태로 복귀한다. 이러한 일련의 과정은, 사용자가 리모트 컨트롤러(300)를 조작한 것 외에는 그 어느 조작도 하지 않은 것으로서, 모든 동작들이 상기 셸 프로그램(293)의 제어에 의해 자동으로 수행된다.

<42> 그리고, 만약 데이터 입력 장치들 중 리모트 컨트롤러(300)를 제외한 다른 입력 장치의 입력에 의해 정규상태로의 전환이 이루어지는 경우, 상기 OS 프로그램(295)은 모니터(120) 화면에 암호를 입력하라는 메시지를 디스플레이 한다. 이 때 사용자는 키보드(100)를 통해 암호를 직접 입력하며, 입력된 암호는 상기 OS 프로그램(295)에 의해서 미리 설정되어있는 암호와 일치하는지 여부를 판별한다. 그리고, 설정된 암호와 입력된 암호가 서로 일치하면 컴퓨터의 전원 상태는 정규상태로 복귀된다.

<43> 도 7은 본 발명에 의한 컴퓨터 시스템의 전원 상태가 대기상태에서 정규상태로 복귀될 때 수행되는 암호확인 동작 수순을 보여주는 흐름도이다. 도 7을 참조하면, 단계 S100에서, 소정의 시간 동안 데이터가 입력되지 않았는지 여부를 판별한다. 판별 결과 만약 소정의 시간 동안 데이터가 입력되지 않았으면 수순은 단계 S110으로 진행하여 OS 프로그램이 지원하는 화면보호기능을 수행한다.

<44> 이어서, 단계 S120에서는 소정의 시간 동안 데이터가 입력되지 않았는지 여부를 다시 한번 판별한다. 판별 결과 만약 소정의 시간 동안 데이터가 입력되지 않았으면 수순

단계를 단계 S130으로 진행하여 컴퓨터 시스템의 전원 상태를 대기상태로 전환한다.

그리고, 단계 S120에서의 판별 결과 만약 소정의 시간 동안에 데이터가 입력되었다면, 수순은 다음 질문을 위한 단계 S150으로 진행한다. 단계 S150에서는, 입력된 데이터가 리모트 컨트롤러로부터 입력된 것인지 여부를 판별한다. 판별 결과, 만약 입력된 데이터가 리모트 컨트롤러로부터 입력되었다면, 수순은 단계 S160으로 진행하여 암호 자동 입력 및 확인 기능을 수행한다. 이는 암호확인 기능을 수행하는 OS 프로그램으로 셀 프로그램이 직접 리모트 컨트롤러로부터 입력된 암호를 전달함으로써 이루어진다. 단계 S160에서의 암호 자동 입력 및 확인이 종료되면 단계 S200에서 정규 상태로 복귀된다.

<45> 상기 단계 S150에서의 판별 결과, 만약 입력된 데이터가 리모트 컨트롤러로부터 입력되지 않았다면, 수순은 단계 S170으로 진행한다. 단계 S170에서, 암호확인 기능을 수행하는 OS 프로그램은 암호를 입력하라는 메시지를 모니터 화면에 디스플레이 한다. 이어서 단계 S180에서 사용자는 키보드와 같은 입력 장치를 통해 암호를 입력한다. 그리고 단계 S190에서는 입력된 암호와 설정된 암호를 확인하고, 두 암호가 일치하는 것으로 판별되면 단계 S200에서 정규 상태로 복귀된다.

<46> 그리고, 상기 단계 S130에서 컴퓨터 시스템의 전원이 대기상태로 전환된 후, 수순은 단계 S140으로 진행하여 소정의 시간 동안 데이터가 입력되지 않았는지 여부를 다시 한 번 판별한다. 판별 결과, 만약 소정의 시간 동안 데이터가 입력되지 않았으면 단계 S130으로 되돌아가서 컴퓨터 시스템의 전원 상태를 대기상태로 유지한다. 단계 S140의 판별 결과 만약 소정의 시간 동안 데이터가 입력되었으면 수순은 단계 S150으로 진행하여, 앞에서 설명한 바와 같이 입력 장치의 종류에 따른 암호확인 단계를 수행한다.

<47> 앞에서 설명한 바와 같이, 대기 상태에서 정규 상태로의 컴퓨터 시스템의 전원 상

태 전환이 리모트 컨트롤러의 데이터 입력에 의해 실행되면, 셸 프로그램은 리모트 컨트롤러로부터 전송되는 암호를 OS 프로그램에 자동으로 입력해준다. 따라서, 사용자가 키보드를 통해 암호를 입력해주지 않아도 상기 셸 프로그램에 의해서 암호가 자동으로 입력되는 자동 암호 확인 기능이 수행된다. 그 결과, 사용자는 훨씬 간편한 방법으로 암호 확인 과정을 수행할 수 있다.

<48> (실시예 2)

<49> 다음은 본 발명의 제2 실시예를 첨부도면 도 8 내지 도 10을 참조하여 상세히 설명한다.

<50> 본 발명의 제2 실시예는 멀티유저 컴퓨터 시스템을 예로 들어 설명한다. 본 발명의 제2 실시예에 따른 멀티유저 컴퓨터 시스템은 컴퓨터 시스템이 리모트 컨트롤러에 의해 대기상태에서 정규상태로 복귀할 때 암호확인 작업을 자동으로 수행한다. 그러므로 사용자가 키보드와 같은 입력장치를 통해서 입력해야했던 암호입력 작업을 자동으로 수행함으로써 사용자의 편의를 도모할 수 있다.

<51> 도 8은 본 발명의 제2 실시예에 따른 멀티유저 컴퓨터 시스템의 개략적인 구성을 보여주는 블록도이다. 도 8에 도시된 바와 같이, 본 발명의 멀티유저 컴퓨터 시스템(600)은 다수개의 리모트 컨트롤러(700, 710, 720, 730)와 무선으로 접속된다. 다수의 사용자들은 각기 자신의 리모트 컨트롤러(700, 710, 720, 730)를 이용하여 멀티유저 컴퓨터 시스템(600)을 원격으로 제어할 수 있다. 멀티유저 컴퓨터 시스템(600)은 원격 제어 신호 수신부(610), GPIO(620), 셸프로그램(630)을 포함하는 구성으로 원격 제어 신호의 입력을 처리하는 기본적인 동작은 상기 제1 실시예의 컴퓨터 시스템의 구성과 동일하다. 상기 원격제어신호 수신부(610)는 상기 제1 실

시예의 경우와 같이, 마이크로 컨트롤러, EEPROM, 원격제어 신호 수신회로들로

구성된다. 원격제어신호 수신부(610)에 구비되는 EEPROM에는 다중 사용자들의 각각의

패스워드가 저장되어 있으며, 원격제어신호의 입력시 패스워드 확인에 사용된다.

<52> 이하 본 발명의 제2 실시예의 설명은 제1 실시예와 다른 부분 즉, 다수의 사용자로부터 입력되는 원격 제어신호의 입력을 처리하는 방법에 대해서 구체적으로 설명한다.

<53> 도 9는 도 8의 멀티유저 컴퓨터 시스템(600)의 하드디스크의 메모리 영역을 보여주는 도면이다. 도면에 도시된바와 같이, 하드디스크의 메모리 영역(800)은 STD 영역(810)과 일반 영역(820)으로 구분된다. STD 영역(810)은 서스펜드 투 디스크(suspend to disk)시에 메인 메모리(main memory)의 내용이 저장될 영역이다. STD 영역은 멀티유저 수에 해당하는 만큼 동일한 영역들(811, 812, 813, 814)들로 분할되어 있다. 일반 영역(820)은 운영시스템, 어플리케이션 프로그램, 데이터 등이 저장되는 일반적인 하드디스크 저장 영역이다.

<54> 도 10은 도 8의 멀티유저 컴퓨터 시스템(600)의 암호확인 동작 수순을 보여주는 흐름도이다. 도 10에 도시된 암호확인 동작의 제어는 원격제어신호 수신부(610)에 구비된 마이크로 컨트롤러에 의해 수행된다.

<55> 리모트 컨트롤러(700, 710, 720, 730)로부터 원격제어신호가 수신되면, 단계 S300에서 패스워드가 히트되는가를 판단한다. 즉, 수신된 원격제어신호에 등록된 사용자의 패스워드가 포함되어 있는가를 판단한다. 수신된 원격제어신호가 등록된

사용자로부터 입력된 것이면, 단계 S310에서 시스템 상태를 체크한다. 시스템 상태가 정규 상태이면 제어는 단계 S320으로 진행한다. 단계 S320에서는 수신된 원격제어신호가 현재 사용중인 사용자로부터 입력된 것인가를 판단한다. 현재 사용자로부터 입력된 것이 아니면 단계 S330으로 진행하여 원격제어신호 입력을 무시하고, 현재 사용자로부터 입력된 것이면 단계 S340으로 진행하여 원격제어신호에 대응하는 처리를 수행한다.

<56> 시스템이 대기상태이면 제어는 단계 S350으로 진행한다. 단계 S350에서는 현재 사용자인가를 판단한다. 현재 사용자이면 제어는 단계 S360으로 진행하여 시스템을 웨이크-업 시킨다. 현재 사용자가 아니면, 제어는 단계 S370으로 진행하여 현재 사용자에 대한 STD(suspend-to-disk)를 실행한다. 그리고 계속해서, 원격제어신호를 입력한 사용자가 STD 상태의 사용자인가를 판단한다. STD 상태의 사용자인 경우에는 제어는 단계 S390으로 진행하여 시스템을 리즘하고, STD 상태의 사용자가 아닌 경우에는 단계 S400으로 진행하여 시스템을 정상적으로 부팅한다. 시스템이 파워 오프 상태이면 제어는 바로 단계 S400으로 진행해서 시스템을 파워 온 시켜 부팅 되도록 한다. 상기 단계 S360과 단계 S390에서 그리고 단계 S400에서 패스워드 체크 과정은 상술한 제1 실시예에서와 같이 자동으로 입력되어지므로 사용자는 별도의 패스워드 입력과정을 거치지 않게 된다.

<57> 이상에서, 본 발명에 따른 회로의 구성 및 동작을 상기한 설명 및 도면에 따라 도시하였지만 이는 예를 들어 설명한 것에 불과하며 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 다양한 변화 및 변경이 가능함은 물론이다.

【발명의 효과】

<58> 이상과 같은 본 발명에 의하면, 단일 사용자 컴퓨터 시스템이나 멀티유저 컴퓨터 시스템의 경우 리모트 컨트롤러에 의해 동작이 제어될 때 그것들의 암호확인 방법이 될

· 썬 간편해지며, 일일이 사용자가 패스워드를 입력하지 않아도 되는 편리한 컴퓨터 사용
· 환경을 제공한다.

+【특허청구범위】

【청구항 1】

리모트 컨트롤러에 의해 동작이 제어되는 컴퓨터 시스템에 설정된 암호의 확인 방법에 있어서 :

상기 설정된 암호를 확인하는 기능을 시작하기 위한 암호확인 개시 데이터가 발생되는 단계와;

암호확인 수단으로 암호를 입력하는 단계와;

상기 설정된 암호와 상기 입력된 암호가 일치하는지 여부를 판별하는 단계; 그리고

판별 결과, 상기 두 암호가 일치하면 상기 컴퓨터 시스템의 동작 상태를 정규 상태로 전환하는 단계를 포함하며,

상기 입력되는 암호는, 상기 암호확인 개시 데이터가 상기 리모트 컨트롤러에 의해서 발생된 경우, 셀 프로그램에 의해서 상기 암호확인 수단으로 자동으로 입력되는 것을 특징으로 하는 리모트 컨트롤러로 구동되는 컴퓨터 시스템의 자동 암호 확인 방법.

【청구항 2】

제 1 항에 있어서,

상기 암호확인 개시 데이터는, 상기 리모트 컨트롤러, 키보드, 또는 마우스와 같은 데이터 입력 장치들 중 어느 하나에 의해서 발생하는 것을 특징으로 하는 리모트 컨트롤러로 구동되는 컴퓨터 시스템의 자동 암호 확인 방법.

【청구항 3】

제 1 항에 있어서,

상기 리모트 컨트롤러는, 상기 컴퓨터 시스템을 원격으로 제어하기 위한 명령과 암호를 발생하는 것을 특징으로 하는 리모트 컨트롤러로 구동되는 컴퓨터 시스템의 자동 암호 확인 방법.

【청구항 4】

제 1 항에 있어서,

상기 암호를 입력하는 단계는,

상기 암호확인 개시 데이터가 상기 리모트 컨트롤러에 의해서 발생된 경우, 셀 프로그램에 의해 자동으로 수행되며,

상기 암호확인 개시 데이터가 상기 리모트 컨트롤러를 제외한 다른 데이터 입력장치에 의해서 발생된 경우, 키보드를 통해 사용자가 직접 상기 암호를 입력하는 것을 특징으로 하는 리모트 컨트롤러로 구동되는 컴퓨터 시스템의 자동 암호 확인 방법.

【청구항 5】

제 1 항에 있어서,

상기 암호 확인 수단은, 윈도우즈와 같은 OS 프로그램인 것을 특징으로 하는 리모트 컨트롤러로 구동되는 컴퓨터 시스템의 자동 암호 확인 방법.

【청구항 6】

제 1 항에 있어서,

상기 암호를 확인하는 기능은,

상기 컴퓨터 시스템의 절전 및 보안을 위해 제공되며, 상기 컴퓨터 시스템의 전원 상태가 대기상태에서 정규상태로 전환되기 직전에 실행되는 것을 특징으로 하는 리모트 컨트롤러로 구동되는 컴퓨터 시스템의 자동 암호 확인 방법.

【청구항 7】

다수개의 리모트 컨트롤러와 무선으로 접속되는 멀티유저 컴퓨터 시스템의 자동 암호 확인 방법에 있어서:

원격제어신호가 수신될 때, 수신된 원격제어신호가 등록된 사용자의 패스워드를 포함하고 있는가를 판단하는 단계;

등록된 사용자로부터 원격제어신호가 입력되면, 시스템의 상태를 판단하는 단계;

시스템이 정규상태이고, 상기 원격제어신호가 현재 사용중인 사용자로부터 입력된 경우 상기 원격제어신호에 대응하는 제어를 수행하는 단계;

시스템이 대기상태이고, 상기 원격제어신호가 현재 사용중인 사용자로부터 입력된 것이면 시스템을 웨이크 업 시키는 단계;

시스템이 대기상태이고, 상기 원격제어신호가 현재 사용중인 사용자로부터 입력된 것이 아니면, 현재 사용자에 대한 서스펜드 투 디스크(suspend to disk)를 실행하는 단계;

상기 원격제어신호를 입력한 사용자가 서스펜드 투 디스크 상태의 사용자인가를 판단하는 단계;

상기 원격제어신호를 입력한 사용자가 서스펜드 투 디스크 상태의 사용자이면 시스템을 리쥘(resume) 시키고, 그렇지 않으면 시스템을 파워 온 시켜 정상 부팅하는 단계;

시스템이 파워 오프 상태이면 시스템을 파워 온 시켜 정상 부팅하는 단계를 포함하는 것을 특징으로 하는 멀티유저 컴퓨터 시스템의 자동 암호 확인 방법.

【청구항 8】

제 7 항에 있어서,

상기 시스템을 웨이크 업, 리즘, 부팅시키는 각각의 단계는 각 단계에서 수행되는 암호 확인이 자동으로 입력 처리되는 것을 특징으로 하는 멀티유저 컴퓨터 시스템의 자동 암호 확인 방법.

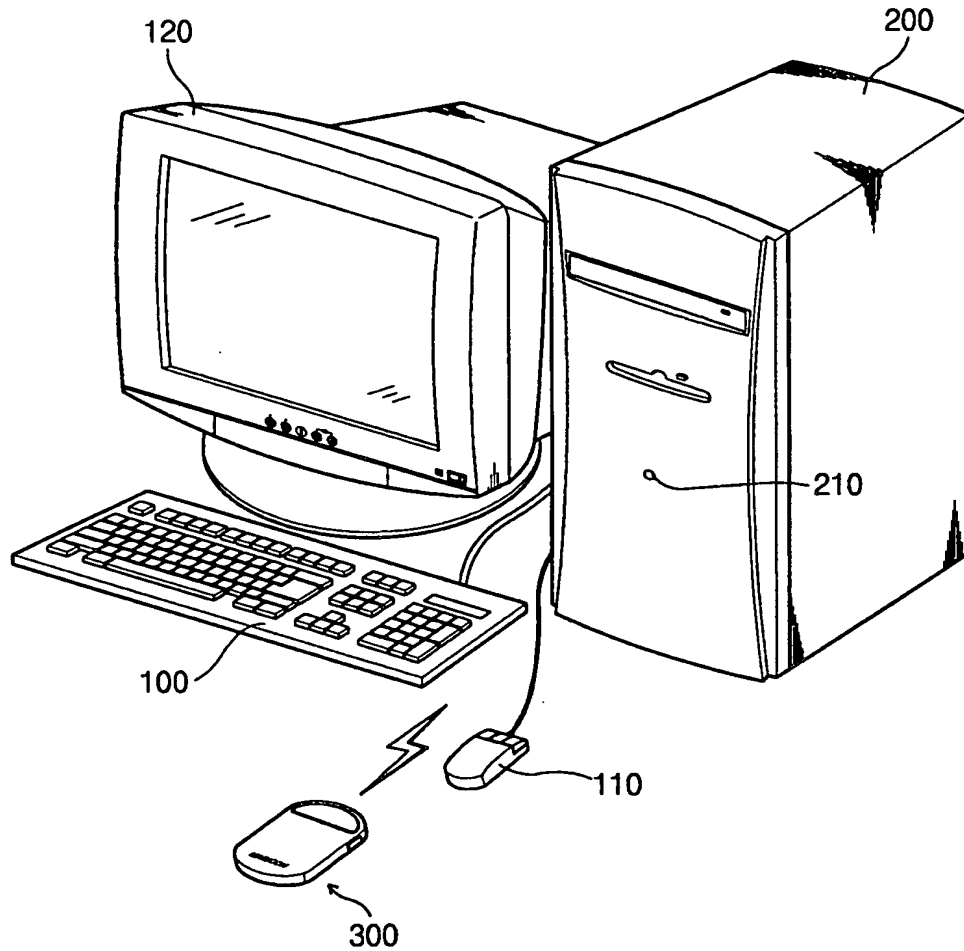
【청구항 9】

제 8 항에 있어서,

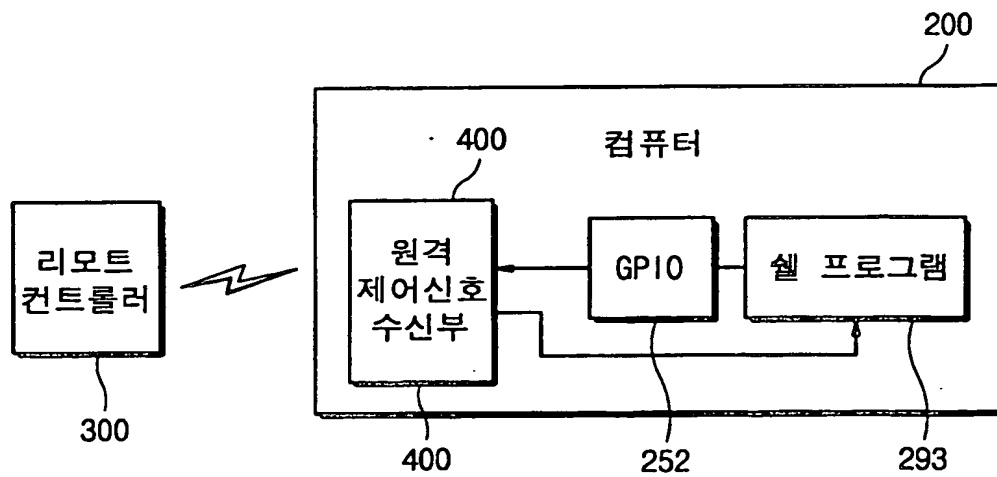
상기 멀티유저 컴퓨터 시스템은 멀티유저 각각에 대한 복수개의 서스펜드 투 디스크 저장 영역을 갖는 하드디스크를 포함하는 것을 특징으로 하는 멀티유저 컴퓨터 시스템의 자동 암호 확인 방법.

【도면】

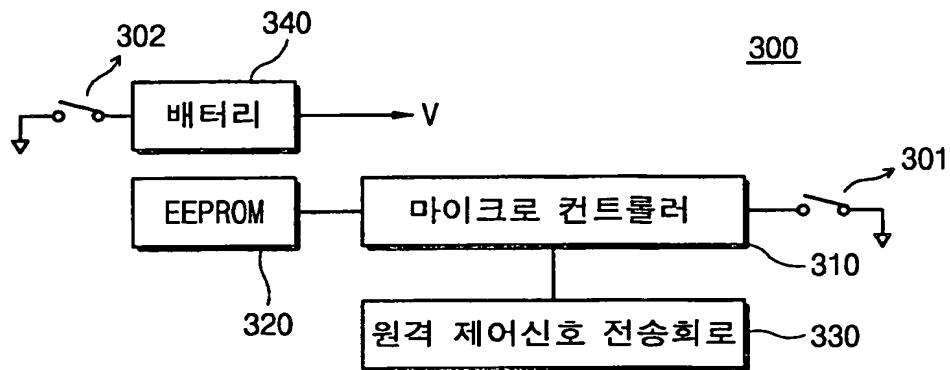
【도 1】



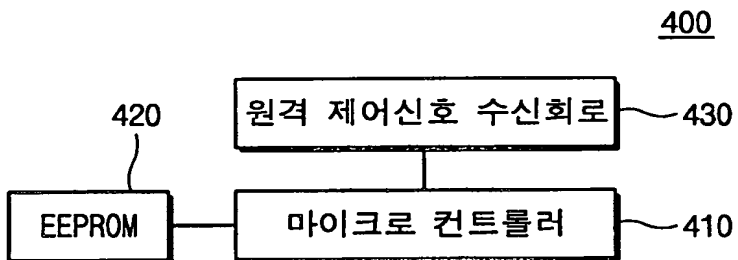
【도 2】



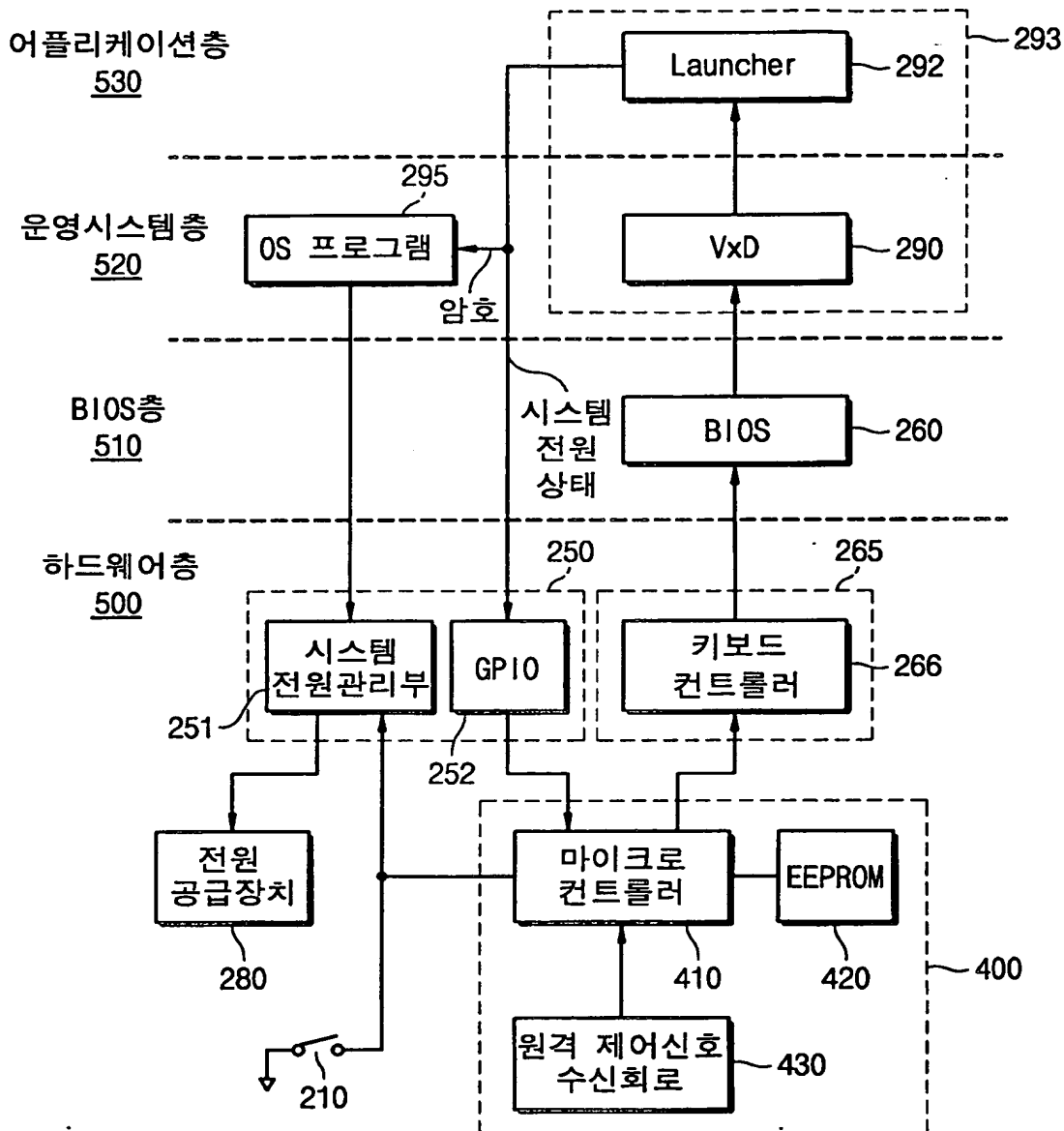
【도 3】



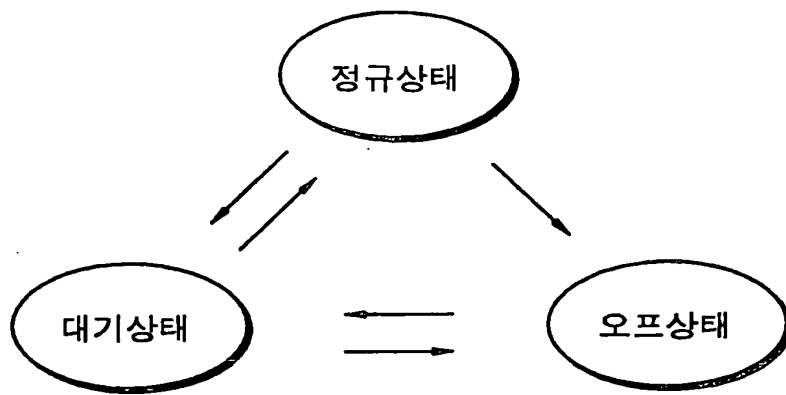
【도 4】



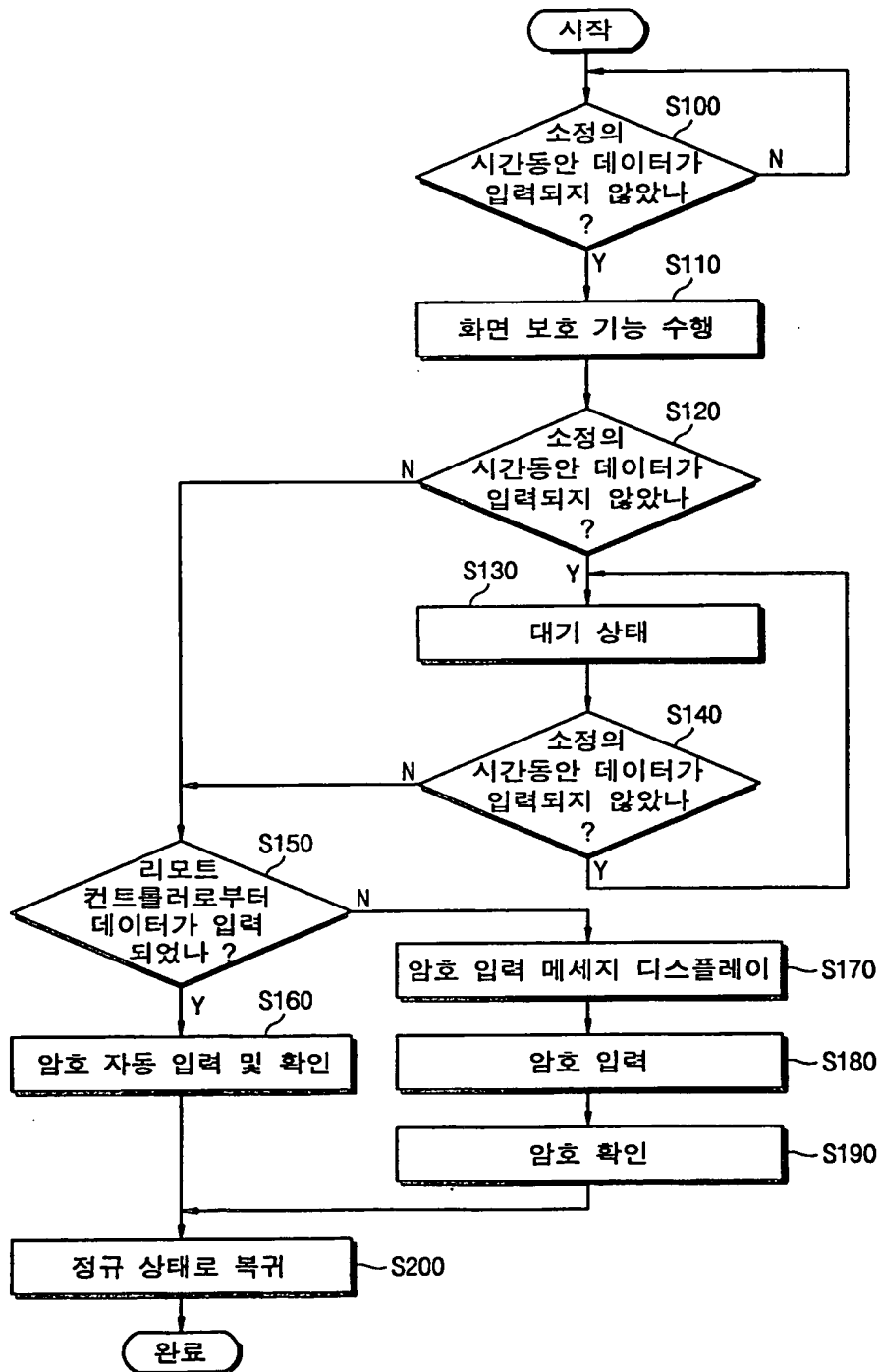
【도 5】



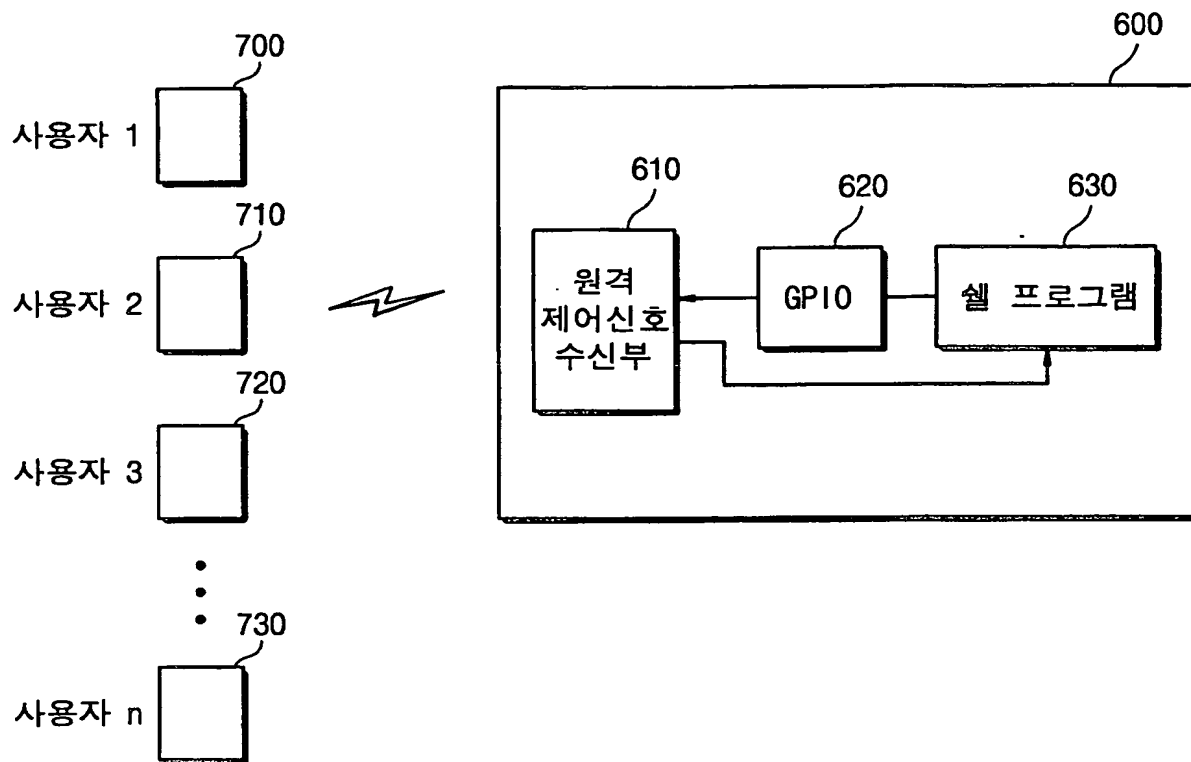
【도 6】



【도 7】

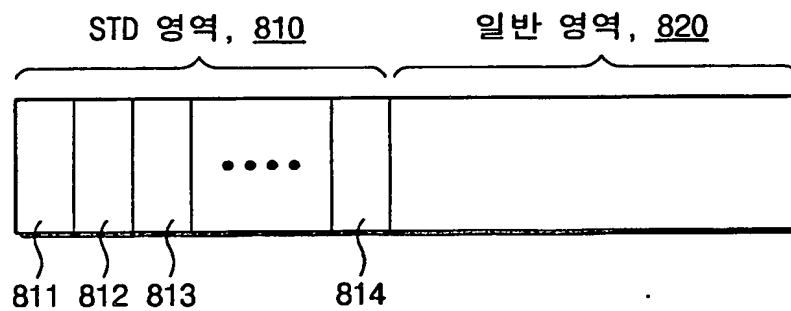


【도 8】



【도 9】

하드 디스크의 메모리 영역 800



【도 10】

